IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	:	
	:	
	:	
v.	:	**CASE NO. 1:21-CR-83-TSE**
	:	
MAJED TALAT HAJBEH	:	
	:	
Defendant.	:	

MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS FISA SEARCH, AND FOR DISCLOSURE OF FISA MATERIALS TO DEFENSE COUNSEL

The Defendant, Majed Talat Hajbeh, by counsel, respectfully submits this memorandum in support of his motion to suppress the interceptions and searches conducted pursuant to the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1802, et seq., and all fruits thereof, and for disclosure of the underlying FISA applications and materials to defense counsel.

BACKGROUND

On December 7, 2020, Majed Hajbeh was arrested pursuant to a Criminal Complaint and Arrest Warrant, charging him with transportation of child pornography, in violation of 18 U.S.C. § 2252(a)(1) and (b)(1). On December 11, 2020, the Government filed a Notice of Intent to Use Foreign Intelligence Surveillance Act Information, pursuant to 50 U.S.C. § 1825(d), notifying the Court of its intent to rely on the results of a "physical search" conducted pursuant to FISA. On April 20, 2021, Mr. Hajbeh was charged in a three-count indictment with possession, receipt, and transportation of child pornography. Dkt. #42. The Government filed a second and identical Notice of Intent to Use FISA Information on May 5, 2021. Dkt. #46. Mr. Hajbeh was arraigned on May 7, 2021, at which time he entered not guilty pleas and requested trial by jury. The case is set for a jury trial to commence on September 14, 2021.

The entire investigation that led to the charges against Mr. Hajbeh began with a "physical search" conducted by FBI agents of a Google Drive account associated with the email address majedhajbeh@gmail.com, pursuant to a Foreign Intelligence Surveillance Act ("FISA") warrant. This is not a case in which the Government observed Mr. Hajbeh sharing child pornography on a peer-to-peer network. Nor is it a case in which an undercover operation on the dark web linked Mr. Hajbeh to the downloading, accessing, or sharing of any such materials. Rather, the record is clear that nothing other than a FISA search prompted the FBI's investigation of Mr. Hajbeh for child pornography offenses, leading to the issuance of subsequent search warrants for Mr. Hajbeh's Google account, WhatsApp accounts, and Apple iCloud accounts, as well as the ensuing search warrants for Mr. Hajbeh's home, car, and person.

The following is a simplified timeline of events leading up to the search and seizure of Mr. Hajbeh's electronic devices and the pending charges:

On March 23, 2020, FBI Special Agent Michael Skapes filed an Affidavit in Support of Applications for Three Search Warrants (No. 1:20-SW-354, et. al) for the following: (1) Google accounts related to majedhajbeh@gmail.com; (2) various WhatsApp accounts; and (3) Apple iCloud accounts related to majedhajbeh@gmail.com (hereafter the "March 23 Search Warrant"). The Affidavit stated:

> Pursuant to an unrelated court-authorized search of the Google Drive associated with Majed Hajbeh's email account **majedhajbeh@gmail.com** for evidence unrelated to child pornography,[1] FBI agents identified images that, based upon my training and experience, appear to contain child pornography. The Google Drive has not been searched for images of child pornography. The images are further described below.

See Exhibit 1 to Mr. Hajbeh's Motion to Suppress Searches, ¶ 3.

[1] This is presumably the FISA "physical search" referenced in the Government's Notice of Intent to Use FISA Information, although nothing in the Notice expressly states as much.

Based on the Government's disclosures, it appears that this "unrelated court-authorized search" was a FISA search of the Google Drive account linked to the majedhajbeh@gmail.com email address. Despite alleging in his Affidavit that the Google Drive "has not been searched for images of child pornography," SA Skapes described in great detail the contents of the three images alleged to contain child pornography that were observed on the Google Drive. *See* Exhibit 1, ¶¶ 15-18. Importantly, those three images were the sole factual basis to support a probable cause determination that evidence of child pornography may be found in the three categories of accounts SA Skapes sought to search pursuant to the March 23 Search Warrant: the Google account, the various WhatsApp accounts, and the iCloud account. The Affidavit provided information tying the accounts sought to be searched to Mr. Hajbeh, and the remainder of the Affidavit provided boilerplate language regarding consumers of child pornography, the types of technologies they often use, and other matters unrelated specifically to the probable cause basis to search the specific accounts at issue. That warrant was granted by the Honorable Michael S. Nachmanoff on March 23, 2020.

On June 17, 2020, SA Skapes filed another Affidavit in Support of Applications for Three Search Warrants (No. 1:20-SW-732 thru 734), this time to search the following: (1) the home of Mr. Hajbeh, (2) Mr. Hajbeh's vehicle, and (3) the person of Mr. Hajbeh (hereafter the "June 17, 2020 Search Warrant"). *See* Exhibit 2 to Mr. Hajbeh's Motion to Suppress Searches. This Affidavit incorporated by reference SA Skapes's March 23, 2020 Affidavit. In addition, SA Skapes provided information from multiple sources, including Comcast, Google, T-Mobile, Amazon, American Express, and physical surveillance records, indicating that Mr. Hajbeh resided at the Hajbeh family residence in Woodbridge, that he had an additional residence in Windsor Mill, Maryland, that he used numerous telephone numbers and electronic devices registered to the

Woodbridge home, that Mr. Hajbeh uses an iPhone and an iPad, and that he owns and uses a Honda Civic. Beyond the boilerplate language found in virtually all search warrants related to child pornography materials, SA Skapes's June 17 Affidavit simply provided evidence that the locations and things sought to be searched and seized were tied to Mr. Hajbeh. Notably missing from the June 17, 2020 Affidavit was any additional evidence regarding the likely existence of child pornography at the Hajbeh home, Mr. Hajbeh's car, or his person, beyond what was previously alleged in the March 23 Affidavit, which, in turn, relied solely on the existence of three images on the Google Drive that was searched pursuant to a FISA warrant, which images SA Skapes alleged "appear[ed] to contain child pornography." Exhibit 1, ¶ 3. The June 17, 2020 Search Warrant was issued by the Honorable John F. Anderson.

On June 23, 2020, a team of at least 50 law enforcement personnel descended on the Hajbeh home in an incredible show of force in order to execute the June 17, 2020 Search Warrant. The facts and circumstances of that search and Mr. Hajbeh's interrogation on June 23 are detailed in Mr. Hajbeh's Memorandum in Support of Motion to Suppress Defendant's Statements. The FBI seized three electronic devices during that search, and those devices were subsequently searched and found to contain child pornography, resulting in the pending charges.

ARGUMENT

As a preliminary matter, disclosure by the Government of the FISA applications and records to defense counsel is necessary for the accurate and fair determination of the legality of the FISA search and surveillance that was the sole factual predicate for all subsequent searches in this case.[2] Without such disclosure, defense counsel will be unable to adequately represent Mr.

[2] The Government has not provided notice that it conducted "electronic surveillance" pursuant to FISA or the FISA Amendments Act. To the extent that the Government did so, Mr. Hajbeh reserves

Hajbeh in connection with this suppression motion, and the Court will not have the benefit of the defense's perspective on important issues relevant to the Court's determination of the lawfulness of the FISA search.

For the reasons provided below, the images searched pursuant to the FISA warrant, and all fruits thereof, should be suppressed because the surveillance was conducted in violation of FISA, as well as the Fourth Amendment. To be clear, this motion is limited in what defense counsel can argue because the underlying FISA applications and authorizations have not been disclosed. Accordingly, this memorandum provides an outline of legal objections for the Court's consideration in reviewing the FISA materials.

A. Background

Congress enacted FISA in 1978 in response to widespread abuses by federal law enforcement engaged in surveillance for domestic law enforcement purposes.[3] The purpose of this law was to limit such abuses and provide a framework for gathering foreign intelligence while protecting against the use of warrantless surveillance for domestic law enforcement. *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (*en banc*), *vacated on other grounds*, 543 U.S. 1097, 125 S.Ct. 1051 (2005) (FISA established a detailed framework whereby the executive branch "could conduct electronic surveillance for foreign intelligence purposes without violating

---

the right to challenge the results of such surveillance and to request access to the related FISA materials.

[3] *See, e.g.*, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. Rep. No. 94-755, 94th Cong., 2d Sess. (1976); Commission on CIA Activities Within the United States, Report to the President (1975) (commonly referred to as the "Rockefeller Commission Report"). *See also United States v. Belfield*, 692 F.2d 141, 145 (D.C. Cir. 1982) ("[r]esponding to post-Watergate concerns about the Executive's use of warrantless electronic surveillance, Congress, with the support of the Justice Department, acted in 1978 to establish a regularized procedure for use in the foreign intelligence and counterintelligence field").

the rights of citizens."). FISA therefore constituted Congress' attempt to balance the "competing demands of the President's constitutional powers to gather intelligence deemed necessary to the security of the Nation, and the requirements of the Fourth Amendment." H.R. Rep. No. 95-1283, at 15; *see also In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (FISA "was enacted in 1978 to establish procedures for the use of electronic surveillance in gathering foreign intelligence information. . . . The Act was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties") (quotation omitted).

The legal standards for the issuance of a search warrant pursuant to the Fourth Amendment are significantly different from the standard for a FISA physical search warrant. FISA's "probable cause" requirement is simply that the surveillance target is an "agent of a foreign power," that the premises or property to be searched contains foreign intelligence information, and that the premises or property to be searched is owned, used, possessed, or is in transit to or from a foreign power or agent thereof. 50 U.S.C. § 1823(a). In other words, no probable cause that a crime has been, or is being, committed, is required for a FISA warrant. On the other hand, the Supreme Court has often reiterated the long-standing rule that criminal probable cause requires "a reasonable ground for belief of guilt," and that "the belief of guilt must be particularized with respect to the person to be searched or seized." *Maryland v. Pringle*, 540 U.S. 366, 371 (2003). Under FISA, however, unlike with respect to a traditional warrant, the probable cause standard is focused not on the target's alleged commission of a crime, but rather the target's alleged status as "a foreign power or an agent of a foreign power."

Unlike Fourth Amendment search warrants, which are authorized by Magistrate Judges based on probable cause that a crime has been or is being committed, a FISA warrant aims to collect surveillance on foreign intelligence targets, and those warrant applications are reviewed by

the Foreign Intelligence Surveillance Court ("FISC"). *See* 50 U.S.C. §§ 1802(b), 1803, and 1804. The statute requires the Attorney General to review the application for a FISA warrant to determine if it satisfies the criteria in the FISA statute. 50 U.S.C. § 1823(a).

In reviewing such an application, the FISC must reject the application unless it meets the following criteria necessary to make the findings required by § 1823(a):

(i) that the application was made by a federal officer and personally approved by the Attorney General;

(ii) that the identity or description of the target of the search, and a description of the premises to be searched is provided;

(iii) that there exists probable cause to believe

(A) that the target of the physical search is a foreign power or agent thereof;
(B) that the premises or property to be searched contains foreign intelligence information; and
(C) the premises or property is or is about to be owned, used, possessed by, or in transit to or from a foreign power, or an agent of a foreign power;

(iv) that the proposed minimization procedures meet the definition of minimization procedures under §1823(a)(4);

(v) that a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted is provided;

(vi) that the application contains all required statements and certifications under § 1823(a)(6); and

(vii) that a statement of the facts concerning all previous applications that have been made to any judge involving any of the persons, premises, or property specified in the application is disclosed.

If the surveillance target is a "United States person," the FISC is required to determine if the certifications under §1823(a)(6) are "not clearly erroneous." Under 50 U.S.C. § 1825(f), any person who is an "aggrieved person" against whom evidence obtained or derived from a physical search is to be introduced or otherwise used or disclosed in any trial or proceeding may move to suppress the evidence derived from such search on one of two grounds: (1) that the information

was unlawfully acquired; or (2) the physical search was not made in conformity with an order of authorization. An "aggrieved person" means "a person whose premises, property, information or material is the target of physical search or any other person whose premises, property, information, or materials was subject to physical search." 50 U.S.C. § 1821(2).

In addition, FISA outlines the procedures for the Court's review of the FISA applications and authorizations, and for the disclosure of such documents to defense counsel:

> Whenever a court or other authority is notified pursuant to subsection (d) or (e), or whenever a motion is made pursuant to subsection (f), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to a physical search authorized by this subchapter or to discover, obtain, or suppress evidence or information obtained or derived from a physical search authorized by this subchapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and *ex parte* the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search.

50 U.S.C. § 1825(g).

In light of the Government's notices of its intent to rely on evidence against Mr. Hajbeh obtained through "physical searches" pursuant to a FISA warrant, Mr. Hajbeh is clearly an "aggrieved person" with standing to challenge the FISA surveillance and to request the disclosure of the FISA materials to defense counsel for purposes of fully litigating the constitutionality and legality of the subsequent searches that were premised entirely on the FISA search.

B. The Court Should Suppress All Evidence Obtained Pursuant to the FISA Warrant.

The search of Mr. Hajbeh's Google Drive in this case was conducted without probable cause to believe that criminal conduct had occurred or that evidence of criminal activity would be found. Although Mr. Hajbeh is an "aggrieved person" under § 1821(2), he and defense counsel do not have the benefit of the FISA applications that resulted in the searches at issue to fully assess the validity of the application and the Government's compliance with the FISA warrant.

While Mr. Hajbeh is moving the Court to suppress the evidence obtained through FISA, and to disclose the FISA documents to defense counsel, the FISA statute provides that if the Attorney General files an affidavit that "disclosure or an adversary hearing would harm the national security of the United States," the court deciding the motion must consider the application and order for a physical search *in camera* to determine whether the surveillance was lawful. 50 U.S.C. § 1806(f). Accordingly, FISA "requires the judge to review the FISA materials *ex parte in camera* in *every* case" to "decide whether any of those materials must be disclosed to defense counsel." *United States v. Daoud*, 755 F.3d 479, 482 (7th Cir. 2014).

The statute further provides: "In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search." 50 U.S.C. § 1825(g). If the Court determines that the physical search was not lawfully authorized or conducted, "it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the physical search was

lawfully authorized or conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." 50 U.S.C. § 1825(h).

Given the inability of defense counsel to review the FISA materials at this stage, as the Fourth Circuit has acknowledged in similar contexts, the defendant's burden to be particular in providing the basis for his suppression motion must be relaxed because the evidence at issue is held exclusively by the Government. *See United States v. Moussaoui*, 382 F.3d 453, 472 (4th Cir. 2004) (citing *United States v. Valenzuela-Bernal*, 458 U.S. 858, 870-71, 873 (1982)).

In reviewing the FISA applications *in camera* as provided by the statute, this Court must determine, *de novo*, whether the FISA applications complied with the statutory framework described above, and whether the Government complied with the FISA warrant. *See United States v. Hassan*, 742 F.3d 104 (4th Cir. 2014). Among the factors for the Court's consideration are whether there was probable cause as required by FISA, whether the information that led to the FISA applications was lawfully obtained, whether the probable cause determination by the FISC was based on protected First Amendment activity, whether the FISA applications contained any intentional or reckless falsehoods or omissions in violation of *Franks v. Delaware*, 438 U.S. 154 (1978), whether the collection of foreign intelligence was not a "significant purpose" of the FISA warrant, whether all of the certifications required by statute were included in the applications, and whether the Government complied with the terms of the FISA search authorization.

a. *Lack of Probable Cause Under the FISA Standard*

The FISC was required, prior to issuing the FISA warrant for a physical search, to make a finding that there is probable cause to believe that the target of the physical search is a foreign power or agent thereof; that the premises or property to be searched contains foreign intelligence

information; and the premises are or are about to be owned, used, possessed by, or in transit to or from a foreign power, or an agent of a foreign power. 18 U.S.C. § 1823(a).

In this case, we know that the Government searched Mr. Hajbeh's Google Drive account without a Fourth Amendment or Title III-compliant warrant. The Government therefore bears the burden of establishing that Mr. Hajbeh was an "agent of a foreign power" at the time of the FISA applications. An "agent of a foreign power" is defined in § 1801(b) to include any person other than a United States person who knowingly engages in one of the acts named in the statute, such as acting on behalf of a "foreign power," knowingly engaging in international terrorism or activities in preparation thereof, or knowingly engaging in proliferating weapons of mass destruction. The statute also defines as "agent[s] of a foreign power" any person who knowingly engages in clandestine intelligence gathering on behalf of a foreign power, knowingly acts at the direction of a foreign intelligence service, knowingly engages in sabotage or international terrorism, or knowingly enters the U.S. under a false identity on behalf of a foreign power. 18 U.S.C. § 1801(b); § 1821(1).

To the extent the Government alleged in the FISA applications that Mr. Hajbeh was the target of the search and falls within the definition of an "agent of a foreign power," or if the target was a third-party alleged to have owned or possessed Mr. Hajbeh's Google Drive account, the Government was required to present evidence to the FISC to support a finding that Mr. Hajbeh, or the third-party target, *knowingly* engaged in the relevant conduct that falls within the statutory definition of an "agent of a foreign power." This is particularly important in this case, where the apparent target of the search was inside the United States, and the account searched was also located within the United States.

b. *Whether the Information Leading to the FISA Application Was Lawfully Obtained and Was Reliable*

The Court should also evaluate whether the FISA applications were based upon lawfully-obtained information, as well as the reliability of such information. Given defense counsel's inability to challenge the accuracy or reliability of the information that was relied upon to obtain the FISA applications, it is critical that the Court be cognizant of those issues in reviewing the FISA materials. For example, unlike traditional law enforcement information, foreign intelligence information often consists of "raw intelligence", which may not be vetted in the same manner as information collected for domestic law enforcement purposes. In addition, the motivations of the providers of such information may not be as clear as in the context of regular criminal investigations, raising additional concerns about the reliability of such sources of information.

Furthermore, particularly in light of the opacity and secretiveness of the FISA process, there is a greater danger that information in the FISA applications was obtained via unlawful methods, such as warrantless wiretapping or other warrantless electronic surveillance. The Government should thus be required to disclose to the Court whether any of the information that led to the factual basis for the FISA applications was itself obtained from any unlawful means. The Government should likewise be ordered to disclose whether any of Mr. Hajbeh's communications were intercepted under the Terrorist Surveillance Program, a warrantless wiretapping program that was instituted in 2001, and whether any such communications were part of the FISA applications. In addition, while the Government's Notice discloses that it intends to rely on evidence obtained pursuant to a "physical search" under § 1825, it does not address whether the Government *also* engaged in "electronic surveillance" of Mr. Hajbeh under § 1804, or whether it also relied upon information obtained pursuant to the FISA Amendments Act, 50 U.S.C. § 1881a, in searching Mr. Hajbeh's account(s) or obtaining evidence relied upon in its FISA applications. The Government should therefore be directed to disclose to the Court all authority upon which it

relied in conducting any surveillance or searches of Mr. Hajbeh's communications, property, or accounts without a traditional search warrant.

c. *Whether the Probable Cause Basis of the FISA Application Was Protected Speech*

FISA specifically prohibits the Government from relying solely on First Amendment protected activity in establishing the probable cause necessary for the issuance of a FISA warrant. 50 U.S.C. § 1824(a) ("no United States person may be considered an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States."). To the extent that the Government relied upon such activities in its FISA application, such as speech expressing support of certain causes or groups, distributing information, or otherwise engaging in free speech activities, the Court should determine whether the issuance of the FISA warrant violated this provision of the statute.

d. *Whether the Required Certifications Were Filed With the Application*

The Court should also review the FISA application to determine whether they contain all the certifications required by Section 1824(a)(6), which requires a certifying official to certify the following to the FISC:

> (A) that the certifying official deems the information sought to be foreign intelligence information;
> (B) that a significant purpose of the search is to obtain foreign intelligence information;
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
> (D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of Title 50; and
> (E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D)

50 U.S.C. § 1823(a)(6).

The Court should also analyze all FISA applications and orders in this case to determine if there were any lapses between the orders during which surveillance continued, and whether the

Government conducted any searches or surveillance outside of the timeframe permitted by a FISA warrant. *See* § 1824(d) (providing time limits on FISA warrants).

e. ***Whether the Collection of Foreign Intelligence Was Not a "Significant Purpose"***

The Government has not charged Mr. Hajbeh with any offenses related to espionage, terrorism, or any of the other grounds for which he may be deemed to be an "agent of a foreign power." Regardless of whatever suspicions the Government may have had, or may currently have, of Mr. Hajbeh, and for which the Government has expended significant resources to surveil and investigate him, he has only been indicted on charges related to child pornography, not charges implicating national security or foreign intelligence gathering. This is despite the significant resources and time the Government has dedicated to surveilling and investigating Mr. Hajbeh. For example, we now know that the FBI placed Mr. Hajbeh under regular physical surveillance for an extended period of time, watching and documenting his most minute of movements. The Government has produced literally hundreds of (redacted) pages of physical surveillance logs, indicating that the FBI has been physically surveilling Mr. Hajbeh since *at least* February 2020 (at least according to the surveillance logs that have been produced to date). The Government has also interviewed dozens and dozens of individuals with close and tenuous connections to Mr. Hajbeh, in addition to subpoenaing virtually all of his online, banking, credit card, cellphone, and other accounts as early as the summer of 2019. Despite all of this, the Government has not charged Mr. Hajbeh with anything other than violations of domestic criminal laws related to child pornography.[4]

[4] There is also no allegation by the Government that Mr. Hajbeh shared or distributed any child pornography materials with any non-U.S. person. Indeed, the "transportation" charge in this case stems from the Government's allegation that Mr. Hajbeh transferred the visual depictions to *himself* from one account to another. The Government has only alleged a single incident in which

If the Government's investigation, and the purpose of its FISA search, was criminal in nature, all the evidence obtained as a result of the FISA search must be suppressed because the applications did not adhere to FISA's requirements, and the Government did not seek the proper authority to conduct its surveillance under Title III. In this case, particularly given the apparently targeted nature of the Government's investigation of Mr. Hajbeh, it appears highly likely that the Government did not have as a "significant purpose" the collection of foreign intelligence, or that the Government engaged in one of the violations of FISA addressed *infra* in subsection (f) of this memorandum, such as using FISA for purposes of conducting a domestic criminal investigation.

f. *Whether any Reckless or Intentional Falsehoods Were Made and Whether the Government Complied with the FISA Warrant*

As discussed above, without the benefit of the FISA applications, the defendant cannot identify any specific falsehoods or material omissions that may have been made in the FISA applications. *See Daoud*, 755 F.3d at 493 (Rovner, J., concurring) (discussing the difficulty of reconciling *Franks* with denying access to FISA warrant applications, and concluding that "[w]ithout access to the FISA application, it is doubtful that a defendant could ever make a preliminary showing sufficient to trigger a Franks hearing."). Under *Franks v. Delaware*, 438 U.S. 154 (1978), if a defendant makes a "substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statements necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Id.* at 156-57. That case also provides for suppression of evidence following such an evidentiary hearing.

---

a visual depiction was sent to a third party (among videos of adult pornography), and that third party is a U.S.-person.

Despite the inability of defense counsel to point to specific falsehoods or omissions at this stage, counsel notes the possibility of a *Franks* violation in the FISA applications for the Court's consideration in reviewing the FISA materials. Vigilance for such falsehoods or material omissions, as well as any excesses or failures to comply in the Government's execution of the FISA warrant, is critically important, particularly in light of the Government's history of abusing the FISA process, as well as recent disclosures by the Foreign Intelligence Surveillance Court that demonstrate the systemic misuse by the FBI of the FISA process.

As early as 2002, in the case of *In re All Matters Submitted to the Foreign Intelligence* Court, 218 F. Supp. 2d 611, 620-21 (FISC), *rev'd on other grounds sub nom., In re Sealed Case*, 310 F.3d 717 (FISCR 2002), the FISC reported that starting in March 2000, the Department of Justice had come "forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States. The errors related to misstatements and omissions of material facts," including:

- the Government's failure to apprise the FISC of the existence and/or status of criminal investigations of the target(s) of FISA surveillance; and
- improper contacts between criminal and intelligence investigators with respect to certain FISA applications. *Id.*

A later report by the DOJ Inspector General issued on March 8, 2006 demonstrated that these serious violations were neither isolated nor exceptional: the IG concluded that the FBI had found violations of its procedures for intelligence-gathering and wiretapping more than 100 times in the previous two years. *See* Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act, March 8, 2006. Among the violations noted in the report were some that were described as "significant," including "over-collection" (wiretapping that is much broader than

authorized by the FISC), and "overruns" (wiretapping that continued longer than authorized). *Id.* at 24-25.

Based on recent disclosures by the FISC, we now also know that the Government's systematic misuse of the FISA process continues to be a problem today and is far broader than previously known. On April 26, 2021, the Office of the Director of National Intelligence (ODNI) declassified a set of documents related to Section 702 of FISA, which authorizes surveillance without any court approval or suspicion of wrongdoing, but solely to target non-U.S. persons located outside the U.S. and for foreign intelligence reasons only.[5] Among the declassified documents was a November 18, 2020 FISA Court opinion that disclosed shocking problems with the FBI's use of Section 702 to target U.S. persons and to engage in domestic law enforcement.[6] Those violations included, among others:

- Between April 11, 2019 and July 8, 2019, an FBI specialist conducting "limited background investigations" conducted approximately 124 queries of Section 702-acquired information using the names and identifying information of individuals who requested to participate in the FBI's "Citizens Academy" program, as well as other individuals who sought access to an FBI field office. *Id.* at 39.
- Between August 1, 2019 and October 18, 2019, a taskforce officer conducted approximately 69 queries using the names and identifiers of individuals to determine whether the FBI could provide additional information on those persons. *Id.* at 40.

[5] *See* Release of Documents Related to the 2020 FISA Section 702 Certifications, April 26, 2021, *available at* https://www.intelligence.gov/index.php/ic-on-the-record-database/results/1057-release-of-documents-related-to-the-2020-fisa-section-702-certifications.

[6] The FISA Court's opinion is available at https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf

- Additional violations occurred in which the FBI failed to opt out of querying raw FISA-acquired information, as well as conducting overly broad queries.

What is more, the FISA Court found that over the past year, meaning within the timeframe in which Mr. Hajbeh was under investigation by the FBI, "the government has reported numerous incidents involving U.S.-person queries that were designed to return evidence of a crime unrelated to foreign intelligence . . . ." *Id.* at 42. One example cited by the FISC was the discovery during an oversight review that the FBI had conducted 40 queries that were "conducted in support of predicated criminal investigations relating to health-care fraud, transnational organized crime, violent gangs, domestic terrorism involving racially motivated violent extremists, as well as investigations relating to public corruption and bribery." *Id.* "None of these queries," the court found, "was related to national security, and they returned numerous Section 702-acquired products in response." *Id.* Furthermore, the court found that the Government had enabled a search feature permitting law enforcement to conduct "batch" queries using multiple query terms, while simultaneously failing to record whether the query terms were U.S.-person terms, in addition to allowing users to view the contents of Section 702 information without providing a justification in the system. *Id.* at 50.

The 67-page Memorandum and Opinion of the FISA Court details additional problems that appear to be widespread and systemic in nature. These recent disclosures further call for a closer look at every stage of the Government's investigation of Mr. Hajbeh, from the beginning of its investigation, to its application(s) for the FISA warrant(s), to its execution of the warrant(s). Without a careful review, the Court cannot simply trust that the FBI complied with the statutory scheme set forth in the FISA statute and that it complied with the terms of the FISC-issued search authorization.

C. The Court Should Order Disclosure of the FISA Applications to Defense Counsel.

FISA provides that a district court may divulge "portions of the application, order, or other materials relating to the surveillance ... where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f); *see United States v. Rosen*, 447 F.Supp.2d 538, 546 (E.D. Va. 2006). For the reasons stated above, and due to the complexity of the issues presented by the FISA searches at issue, a fair and full assessment of all issues related to Mr. Hajbeh's motion to suppress requires disclosure to defense counsel—under appropriate controls and procedures—the FISA application materials and orders that led to this investigation and the ensuing prosecution.

CONCLUSION

The issues before this Court in this motion are critically important. They implicate the constitutional right of Mr. Hajbeh to be free of unreasonable searches and seizures that violate the Fourth Amendment, as well as the important statutory safeguards enacted by Congress to protect against the use of foreign intelligence gathering as a pretext for domestic law enforcement without probable cause that a crime was committed. The history of past Government excesses and misuses of FISA raise serious concerns about the Government's compliance with the statute and require vigilance by the courts in ensuring that the Government's conduct is scrutinized to ensure full compliance with FISA and the Fourth Amendment.

For the above reasons, and the additional reasons to be provided at such time as counsel may be heard, the Defendant, Majed Hajbeh, by counsel, moves the Court to suppress all evidence obtained as a result of any physical searches or electronic surveillance pursuant to any FISA authorization, and for disclosure to defense counsel of all FISA applications and orders relevant to this prosecution.

Respectfully Submitted,
Majed Talat Hajbeh
By Counsel

ELSAYED LAW PLLC

BY: ____/s/_____

Muhammad Elsayed
Virginia Bar No. 86151
1934 Old Gallows Road
Suite 350
Vienna, Virginia 22182
(703) 884-2636
(703) 884-2637 (fax)
me@elsayedlaw.com

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing pleading was filed electronically using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

____/s/_____
Muhammad Elsayed
Virginia Bar No. 86151
Elsayed Law PLLC
1934 Old Gallows Road
Suite 350
Vienna, Virginia 22182
(703) 884-2636
(703) 884-2637 (fax)
me@elsayedlaw.com